Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

~ Google Scraps Barges! ~ People Are Talking! ~ Tor Project Puzzled!
~ Hacker: Weak Password! ~ Facebook’s "Unfollow"! ~ New Raspberry Pi Out!

~ People Losing Control? ~ WireLurker Is Limited! ~ Facebook To Be Video?
~ More Facebook Privacy? ~ Unicorn Bug Since 1995 ~ Firefox Turns 10!

-* US Falls Behind in Internet? *-
-* "Atari Dump" Documentary To Be Free *-
-* Obama Calls for Tougher Internet Regulation *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""

Well, the "Polar Vortex" is firmly in place here in New England! While this is not an unusual phenomenon, it is making national news. Yes, the cold air has dropped down to the "Lower 48". Yes, parts of the country have been hit with some snow (yep, we had a little here this morning!). Is this a sign of things to come this winter - who knows?! I hope not; I'd love to experience a fairly mild winter like we did last year, but we'll just have to wait and see! Fortunately, our new oil furnace is working quite well!

Until next time...

=~=~=~=

->In This Week's Gaming Section - Microsoft Files New Battletoads Trademark!
""""""""""""""""""""""""""""""" "Atari Dump" Documentary Will Be Free!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""""

Microsoft Files New Battletoads Trademark

Microsoft has filed a new trademark application for Battletoads, suggesting - but absolutely not confirming - that the Xbox company may be planning to revive the series in some fashion.

The trademark application, spotted by NeoGAF, was filed with the United States Patent & Trademark Office (USPTO) on November 5. It covers "game software" and "online video games."

The Battletoads series was created by British developer Rare, and was originally released for the NES in 1991. Microsoft acquired Rare in 2002, and the Battletoads series has been dormant for years.

Could the trademark application mean Microsoft is looking to bring Battletoads back to modern consoles? Maybe, but Microsoft has not announced any plans to date. Filing a trademark application doesn't guarantee a future game release, as Microsoft could just be protecting the name, should it want to make a new game some day.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

Xbox-Produced "Atari Dump" Documentary Will Be Free

The upcoming Xbox-produced Atari: Game Over documentary, which promises to tell the untold story of Atari and the ill-fated launch of E.T., will premiere next week, and it won't cost you a penny.

Microsoft announced today that the movie will debut November 20 on Xbox 360, Xbox One, and PC through video.xbox.com. It will be free on all platforms; you don't need an Xbox Live Gold subscription.

The movie features interviews with the creator of E.T., Howard Warshaw, other Atari employees. The film will also feature footage from the dig that unearthed the buried copies of the game back in April.

Atari: Game Over was directed by Zak Penn, who has written for movies such as The Avengers, The Incredible Hulk, and various X-Men films.

Some of the excavated E.T. copies were recently sold on eBay, fetching more than $1,500.

Atari: Game Over was developed under the Xbox Entertainment Studios banner, a unit responsible for original Xbox programming. The division was short-lived, as Microsoft recently announced the studio's closure.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Obama Calls for Tougher Internet Regulation

President Barack Obama on Monday embraced a radical change in how the government treats Internet service, coming down on the side of consumer activists who fear slower download speeds and higher costs but angering Republicans and the nation’s cable giants who say the plan would kill jobs.

Obama called on the Federal Communications Commission to more heavily regulate Internet providers and treat broadband much as it would any other public utility.

He said the FCC should explicitly prohibit Internet providers like Verizon and AT&T from charging data hogs like Netflix extra to move their content more quickly. The announcement sent cable stocks tumbling.

The FCC, an independent regulatory body led by political appointees, is nearing a decision on whether broadband providers should be allowed to cut deals with the content providers but is stumbling over the legal complexities.

"We are stunned the president would abandon the longstanding, bipartisan policy of lightly regulating the Internet and calling for extreme" regulation, said Michael Powell, president and CEO of the National Cable and Telecommunications Association, the primary lobbying arm of the cable industry, which supplies much of the nation’s Internet access.

This "tectonic shift in national policy, should it be adopted, would create devastating results," added Powell, who chaired the FCC during the Bush administration until 2005.

Consumer groups and content providers hailed Obama’s move, with Netflix posting to its Facebook page that "consumers should pick winners and losers on the Internet, not broadband gatekeepers."

"Net neutrality" is the idea that Internet service providers shouldn’t block, slow or manipulate data moving across its networks. As long as content isn’t against the law, such as child pornography or pirated music, a file or video posted on one site will load generally at the same speed as a similarly sized file or video on another site.

In 2010, the FCC embraced the concept in a rule. But last January, a federal appeals court struck down the regulation because the court said the FCC didn’t technically have the legal authority to tell broadband providers how to manage their networks.

The uncertainty has prompted the public to file some 3.7 million comments with the FCC more than double the number filed after Janet Jackson’s infamous wardrobe malfunction at the 2004 Super Bowl.

On Monday, Obama waded into the fray and gave a major boost to Internet activists by saying the FCC should explicitly ban any "paid prioritization" on the Internet. Obama also suggested that the FCC reclassify consumer broadband as a public utility under the 1934 Communications Act. That would mean the Internet would be regulated more heavily in the way phone service is.

"It is common sense that the same philosophy should guide any service that is based on the transmission of information whether a phone call, or a packet of data," Obama said.

This approach is exactly what industry lobbyists have spent months fighting against. While Internet providers say they support the concept of an open Internet they want flexibility to think up new ways to package and sell Internet services. And, given the billions of dollars spent to improve network infrastructure, some officials say it’s only fair to make data hogs like Netflix bear some of the costs of handling heavy traffic.

AT&T on Monday threatened legal action if the FCC adopted Obama’s plan, while Comcast Corp. said reclassifying broadband regulation would be "a radical reversal that would harm investment and innovation, as today’s immediate stock market reaction demonstrates." Similar statements were released by Time Warner Cable Inc. and several industry groups including CTIA-The Wireless Association, USTelecom, the Telecommunications Industry Association and Broadband for America.

Many Republicans including House Speaker John Boehner, R-Ohio, and Senate GOP Leader Mitch McConnell of Kentucky sided with industry in denouncing the plan as government overreach.

"’Net Neutrality’ is Obamacare for the Internet," declared Sen. Ted Cruz, R-Texas, a tea party favorite, on Twitter. "The Internet should not operate at the speed of government."

The Internet Association, which represents many content providers like Netflix, Twitter, eBay and Google, applauded Obama’s proposal.

On Monday, as the Standard & Poor’s 500 index edged up slightly, big cable companies slid. Time Warner Cable, Comcast, Cablevision and Charter Communications dropped 2 percent to 4 percent in the hours immediately after the announcement.

FCC Chairman Tom Wheeler, a former industry lobbyist and venture capitalist, has said he is open to using a "hybrid" approach that would draw from both Title II of the 1934 law and the 1996 Telecommunications Act. On Monday, Wheeler said he welcomed the president’s comments, but suggested that his proposal was easier said than done.

"The more deeply we examined the issues around the various legal options, the more it has become plain that there is more work to do," Wheeler said. "The reclassification and hybrid approaches before us raise substantive legal questions. We found we would need more time to examine these to ensure that whatever approach is taken, it can withstand any legal challenges it may face."

The FCC isn’t under a deadline to make a decision.

The president’s statement all but guarantees that the major cable companies will spend the next few months trying to encourage Congress to step in to protect their interests. Still, Internet activists are hoping that Obama’s position will go a long way, even as his popularity among his party has waned.

"When the leader of the free world says the Internet should remain free, that’s a game changer," said Sen. Edward Markey, D-Mass.

U.S. FCC Chairman Says ’Must Take The Time’ on Net Neutrality Rules

U.S. Federal Communications Commission Chairman Tom Wheeler on Monday welcomed President Barack Obama’s comments on his work on new Internet traffic, or "net neutrality," rules, saying the agency "must take the time" to set the rules once and for all. Obama on Monday pressured the FCC to toughen its planned Internet traffic rules, saying higher-fee "fast lanes" should be banned and Internet providers should be overseen similarly to public utilities. Wheeler reiterated that he, too, opposed Internet fast lanes or traffic prioritization deals that may harm consumers. "The more deeply we examined the issues around the various legal options, the more it has become plain that there is more work to do," he said in a statement. "The reclassification and hybrid approaches before us raise substantive legal questions. ... We must take the time to get the job done correctly, once and for all, in order to successfully protect consumers and innovators online."

Tech Companies Need To Get Off The Sidelines and Start Loudly Supporting Net Neutrality Right Now

After the president announced his plan to ensure net neutrality by reclassifying broadband providers as utilities, my inbox predictably got flooded with hysterical missives from carriers who are warning that forcing them to abide by net neutrality rules would completely destroy the Internet as we know it. Soon afterward, many congressmen and senators started piling on and declaring that this new net neutrality plan was an Obamacare for the Internet, as Texas Republican Ted Cruz put it.

If things keep playing out this way, then everyone in America will soon see this story as one of the government wanting to control a vital industry just for the sake of exerting its own power. This would be tragic because net neutrality isn t really an issue of government-versus-business so much as it s an issue of business-versus-business.

Or more specifically, it s an issue of whether one kind of business can use its unique economic leverage to extract added rents from another type of business in exchange for giving its traffic priority treatment, which would also put smaller tech companies that can t afford fast lane fees at a permanent disadvantage.

The good news here is that there are many high-profile businesses who have claimed in the past to support strong net neutrality rules since they re not eager to pay ISPs extra tolls in exchange for preferential treatment. And by high-profile, I m referring to Google, Apple, Microsoft, Facebook, Amazon, Netflix and many, many more.

If any plan to implement net neutrality regulations is to survive the barrage of propaganda that s going to be leveled against it, then these tech firms need to speak up and make their voices heard on this matter right now and explain to their users why net neutrality is so important to the future of the online economy.

And let s be clear: If these companies came together to put even a fraction of the effort into supporting net neutrality that the big telcos and cable companies are putting into killing net neutrality, then they would almost certainly win in the court of public opinion.

Why? Because most tech companies are loved by their customers while most wireless and (especially) cable companies are not. In a battle over public trust, the people who bring you your iPhone, your Xbox, Google Maps and Amazon Prime are going to demolish the people who slap you with overage fees for exceeding monthly data caps and who employ customer service representatives that are only slightly less terrifying than Buffalo Bill in Silence of the Lambs.

So now is the time to start putting your considerable money where your mouths are, tech companies. Because if you don t, you ll soon be cursing your fate every time you have to pay Comcast a paid prioritization fee to ensure your traffic gets delivered as quickly as your rivals does.

FCC May Give Us Internet Fast Lanes No Matter What Obama Says

President Obama this week caused quite a stir when he came out in favor of a bold plan to protect net neutrality that would involve reclassifying ISPs as common carriers. Unfortunately for net neutrality advocates, Obama doesn t get the final say when it comes to this issue. Instead, that honor goes to the Federal Communications Commission, which is headed by a former cable lobbyist that Obama decided to appoint as chairman last year.

The Washington Post brings us word that Obama s newly unveiled net neutrality plan isn t going to change what the FCC does one bit and that the commission might just go through with its plan to allow ISPs to charge more money to companies to make sure their traffic gets delivered faster no matter what.

 Huddled in an FCC conference room Monday with officials from major Web companies, including Google, Yahoo and Etsy, agency Chairman Tom Wheeler said he preferred a more nuanced solution, the Post reports. His approach would deliver some of what Obama wants but also would address the concerns of the companies that provide Internet access to millions of Americans, such as Comcast, Time Warner Cable and AT&T.

Wheeler also reportedly told these tech companies that he s trying to figure out the best way to split the baby, although that can t be too comforting when the baby being split is the open Internet. The FCC is an independent agency, however, and it s under no obligation to listen to the president, congressmen or anyone else in the government. No matter what anyone wants, the FCC might still give us Internet fast lanes.

People Feel Loss of Control of Personal Info

It’s been 15 years since Sun Microsystems CEO Scott McNealy infamously quipped "You have zero privacy anyway. Get over it." You’d think we would have gotten the message by now, with all the news of online data breaches, revelations about broad government surveillance, and advertisers tracking your every move as you travel around the Web.

But we’re not over it. We just don’t know what to do about it.

That’s the finding of a new Pew Research Center survey, which revealed that nearly all Americans surveyed feel they’ve lost control over how companies collect and use their personal information.

"It’s a trade-off," said Bill Scully, 47, from Boston, while waiting for a train inside New York’s Penn Station. When you sign up for Google Inc.’s Gmail, for example, you get free email in exchange for letting the company target ads to you, he said. "The same with Facebook. When you sign up for Facebook, you are basically signing up for a big marketing survey."

The survey by the Pew Research Center’s Internet Project asked 607 U.S. adults about their privacy perceptions following Edward Snowden’s exposure of government surveillance programs last year. The study found that most have "little confidence" in the security of communications tools ranging from social media sites to phones, and less than a quarter think that it is easy to be anonymous online.

Some 81 percent said they don’t feel secure using social networking sites when they want to share private information. More than half of respondents are insecure emailing or texting private details, such as health issues. And 80 percent of those who use social networking sites like Facebook, Twitter and LinkedIn are concerned about advertisers and businesses accessing the information they share on the sites. Two-thirds of them think the government should do more to regulate those advertisers.

Asked if he feels that his information is secure online, Jeff Ji, from New Jersey, answered with an emphatic "no." He said he has had his credit card information breached, and is familiar with advertisers tracking his movements online. That said, he thinks that people have "no choice in the matter" if they want to use email or social media, even if it means sharing private information.

"Everyone uses it. It’s a huge network and (we) need it to communicate with others," he said.

Since its 2004 launch, Facebook’s user base has skyrocketed to more than 1.35 billion, despite ongoing user concerns about what happens to the vast trove of information that is shared on the site, albeit for free. Facebook uses people’s likes, hometown, hobbies and movements around the Web to target ads to them, though it emphasizes that advertisers aren’t privy to any information that could personally identify a user. Other free sites teeming with personal information include LinkedIn, where 300 million members have filled out pages with employment details and contacts. Users need to take steps to opt out of behavior tracking if they don’t want to receive targeted ads.

Many people are OK with that 55 percent of the survey’s respondents said they are willing to share some personal information so they can use online services for free. "You’re not paying for privacy," notes Priscilla Granger, 28, also from New Jersey. But nearly two-thirds of those polled don’t think giving away all those personal details actually make websites and online services "more efficient." And the same number say they want to make a bigger effort to protect their privacy.

Pew plans to conduct four surveys on the topic over the course of a year. This report is based on the first survey, which was conducted Jan. 11-28 among a representative online panel of 607 adults. Although the panel was conducted online, Internet access was provided to respondents

without it. The sampling error is 3.98 percent.

Americans Leery of Online Privacy in Post-Snowden Era

Ever since NSA whistleblower Edward Snowden began unleashing details of US government surveillance programs, Americans have become increasingly worried about both the government and businesses tracking them online.

That s according to a study published today by the Pew Research Center, which found that a majority of Americans believe their privacy is being challenged and that they are losing the ability to secure their personal information and retain confidentiality.

The survey, which was conducted in January, found that roughly 8 in 10 adults are concerned about the government s monitoring of phone calls and Internet communications, while some 91 percent of adults feel like they ve lost control over how personal information is collected and used by companies.

Social media is no better, as 80 percent of adults say they are worried about the access that advertisers and other companies have to their personal data. Seventy percent of respondents said they worried that government agencies might access and track personal information about them on social networking sites.

But here exists the paradox: More than half of respondents said they were willing to share their personal information in order to use online services for free, even though distrust in advertisers remains widespread.

As for the impact that the Snowden revelations have had on how Americans perceive their privacy, it seems as though the more people know, the more distrust they tend to have.

"Americans' lack of confidence in core communications channels tracks closely with how much they have heard about government surveillance program," the Pew report stated.

Yet in spite of the overall public concern about government surveillance, 64 percent believe the government should do more to regulate advertisers' access to their data online.

Congressional Committee Meeting To Discuss Privacy in Wake of Recent Nude Leaks

A congressional advisory committee will be taking the initial step Thursday to discuss the legal ramifications of protecting Internet privacy. Prompted by the recent hacks resulting in the leak of nude photos of celebrities like the high profile case involving actress Jennifer Lawrence, the Congressional Internet Caucus Advisory Committee will be discussing the topic of privacy and the legal remedies against hackers, websites, and those partaking in revenge porn.

In a session titled "Jennifer Lawrence's Hacked Photos: A "Sex Crime?" The Legal Underpinnings of Digitally Exposed Private Images and What Congress

Needs to Know" the advisory committee, which is comprised of members of the private sector and is not a government body, will be asking what remedies, if any at all, ordinary citizens will have against people who hack, leak, or peddle private photos.

To engage the public and gain coverage, the committee will be using the hashtag #exposedphotos on Twitter, so be sure to join in on the discourse.

Feds Hacked: Is Cybersecurity A Bigger Threat Than Terrorism?

While the terrestrial fears of terrorism and Ebola have dominated headlines, American leaders are fretting about what may be even more serious virtual threat s to the nation s security.

This year, hundreds of millions of private records have been exposed in an unprecedented number of cyberattacks on both US businesses and the federal government.

On Monday, just as President Obama arrived in Beijing to being a week-long summit with regional leaders, Chinese hackers are suspected to have breached the computer networks of the US Postal Service, leaving the personal data of more than 800,00 employees and customers compromised, The Washington Post reports.

The data breach, which began as far back as January and lasted through mid-August, potentially exposed 500,000 postal employees most sensitive personal information, including names, dates of birth, and Social Security numbers, the Postal Service said in a statement Monday. The data of customers who used the Postal Service s call center from January to August may have also been exposed.

"The FBI is working with the United States Postal Service to determine the nature and scope of this incident," the federal law enforcement agency said in a statement Monday. Neither the FBI nor the Postal Service, however, confirmed it was the work of Chinese hackers.

The breach did not expose customer payment or credit card information, the Postal Service said, but hackers did gain access to its computer networks at least as far back as January. The FBI informed the Postal Service of the hack in mid-September.

 It is an unfortunate fact of life these days that every organization connected to the Internet is a constant target for cyber intrusion activity, said Postmaster General Patrick Donahoe in a statement. The United States Postal Service is no different. Fortunately, we have seen no evidence of malicious use of the compromised data and we are taking steps to help our employees protect against any potential misuse of their data.

But the reported breach comes as both intelligence officials and cybersecurity experts say computer hackers now pose a greater threat to national security than terrorists.

Since 2006, cyber-intruders have gained access to the private data of nearly 90 million people in federal networks, the Associated Press reported in a major investigation published Monday.

Hackers have also accessed 255 million customer records in retail networks during this time, 212 million customer records in financial and insurance industry servers , as well as 13 million records of those in educational institutions, the AP reported.

The increasing number of cyber-attacks in both the public and private sectors is unprecedented and poses a clear and present danger to our nation s security, wrote Rep. Elijah Cummings (D) of Maryland, ranking member of the House Committee on Oversight and Government Reform, in a letter to Postmaster General Donahoe on Monday.

Still, unlike the well-publicized hacks of businesses like Home Depot and Target, in which the payment information of nearly 100 million customers was exposed this year, recent data breaches have puzzled experts.

In October, JPMorgan Chase, the largest US bank, reported that hackers had compromised the personal contact information of more than 83 million customers. But even though the hackers, suspected to be from Russia, had access to numerous servers in JPMorgan s systems, they accessed only personal information lists not accounts or financial data.

Russian hackers were also suspected of being behind a breach of unclassified White House computers, reported in October as well.

The limited scope of the information that such hackers gained access to this year may indicate that they are simply exploring system security in the never-ending chess matches of international espionage and spying, experts say.

But the battle against highly sophisticated hackers, cybersecurity experts say, is a 24/7, 365-days-a-year arms race. It s a cat-and-mouse game as hackers constantly probe a network s defenses, finding inevitable flaws and weaknesses that system administrators must patch on a regular, ongoing basis.

This means hackers are usually one step ahead.

"No matter what we do with the technology ... we'll always be vulnerable to the phishing attack and ... human-factor attacks unless we educate the overall workforce," Eric Rosenbach, assistant secretary of Defense for Homeland Defense and Global Security, told the AP.

Tor Project Puzzles Over How The Law Shredded Anonymity in Operation Onymous

When the administrator of Silk Road 2.0 was busted last week, the agent who penned his indictment was tight-lipped about how, exactly, the FBI got its hands on the supposedly hidden server the dark net market was using, saying that the Bureau simply "identified the server located in a foreign country," and that law enforcement managed to image it sometime around 30 May 2014.

In or about May 2014, the FBI identified a server located in a foreign country that was believed to be hosting the Silk Road 2.0 website at the time (the Silk Road 2.0 Server). On or about May 30, 2014, law enforcement personnel from that country imaged the Silk Road 2.0 Server and conducted a forensic analysis of it. Based on posts made to the SR2

Forum, complaining of service outages at the time the imaging was conducted, I know that once the Silk Road 2.0 server was taken offline for imaging, the Silk Road 2.0 website went offline as well, thus confirming that the server was used to host the Silk Road 2.0 website.

That’s it. That’s all that law enforcement was willing to share about how it managed to slice through the layers of the Tor network, which is designed to mask users’ identity by means of software that routes encrypted browsing traffic through a network of worldwide servers.

Now, the keepers of Tor - the nonprofit group The Tor Project - are trying to puzzle out how identities were laid bare in the farflung, multi-nation bust, dubbed Operation Onymous, that snared 410+ supposedly hidden services running 27 markets, including Silk Road 2.0.

The Tor user base doesn’t just include bad guys - the drug lords, drug buyers, illicit arms traffickers, money launderers and child-abuse image swappers.

It also includes activists and others for whom it’s crucial to protect privacy so as to ensure safety from persecution, be it from oppressive regimes or dangerous stalkers.

The Tor Project doesn’t know how the anonymizing service was foiled, but it has possibly relevant information it shared on Sunday.

As Tor project executive director Andrew Lewman wrote, in the previous few days, The Tor Project had received reports that several Tor relays had been seized by government officials (The Tor Project doesn’t know how or why) - specifically, three Torservers.net systems (used to run Tor exit nodes) that blinked out of existence.

The "How" of the onion-router slicing has a few possible avenues of inquiry.

One of those paths involves blaming the unmasked victims themselves for using inadequate operational security.

This is "the first and most obvious explanation", writes Tor project executive director Andrew Lewman:

The project has received reports about websites being infiltrated by undercover agents, while [Benthall’s indictment] states various operational security errors.
Other possibilities Lewman suggested:

SQL injection. Lewman notes that many of the sites discovered in Operation Onymous were likely "quickly-coded e-shops with a big attack surface" that could well have been vulnerable to SQL injection.

Bitcoin de-anonymization. Recent research from Cornell University describes a way to de-anonymize Bitcoin users that allows for the linkage of user pseudonyms to the IP addresses from which the transactions are generated, even when used on Tor.

Attacks on the Tor network. Given the number of takedowns and the seizure of Tor relays, the Tor network was possibly attacked to reveal the location of the hidden services. Lewman lists a number of attacks that have been discovered on the Tor network over the past few years - attacks with the potential aftermath of de-anonymizing previously hidden

services.

In fact, two Carnegie Mellon researchers canceled a Black Hat 2014 talk about how easy they found it to break Tor.

The researchers claimed that it was possible to "de-anonymize hundreds of thousands of Tor clients and thousands of hidden services within a couple of months," and promised to discuss examples of their own work identifying "suspected child pornographers and drug dealers."

From the original description, before Carnegie-Mellon’s lawyers had the talk yanked from the lineup:

There is nothing to prevent you from using your resources to de-anonymize the network’s users ... by exploiting fundamental flaws in Tor design and implementation. And you don’t need the NSA budget to do so.

Looking for the IP address of a Tor user? No problem. Trying to uncover the location of a hidden service? Done. We know because we tested it, in the wild...

At the time, The Tor Project confirmed that yes, somebody or somebodies were picking it apart, and the assaults may have unmasked those who run or visit Tor-hidden sites.

In the meantime, Lewman asks relay operators to get in touch if their server was recently compromised or they lost control of it.

FBI Most Wanted Hacker Jeremy Hammond Used His Cat’s Name for Password

A notorious hacker serving a federal prison sentence revealed that a weak password - his cat’s name - may have led to his downfall.

Jeremy Hammond, who is serving a 10-year prison sentence for his role in cyber attacks against a private defense firm, law enforcement agencies and what prosecutors called "thousands of innocent individuals," was able to hack into systems that may have seemed impenetrable to others.

It would be fair to expect a hacker as skilled as Hammond to keep his private information carefully protected, but instead he told the Associated Press he used a password that was surprisingly easy: Chewy 123.

"My password was really weak," he told the AP.

Hammond said he still isn’t sure how federal authorities were able to get into his encryption program and gather evidence that ultimately sent him to prison, however, he said he wonders if his weak password may have been the culprit.

The "hacktivist" portrayed his actions as acts of civil disobedience, but at his sentencing last year Judge Loretta Preska of the U.S. District Court for the Southern District of New York said Hammond "hacked into websites he disagreed with politically."

Facebook Again Tries To Simplify Privacy Policy

One more time, Facebook is trying to simplify its lengthy privacy policy and make it much shorter to explain how it targets advertisements to its 1.35 billion users.

The world's largest online social network uses the information people share on its site, along with the apps they use and the outside websites they visit, to show them advertisements deemed relevant to them. In the July-September quarter, Facebook reported nearly $3 billion in advertising revenue, a 64 percent increase from a year earlier.

Over the years, the company has faced concerns from users and from government regulators and privacy advocates that its policies are too complicated. Two years ago, it settled with the Federal Trade Commission over charges that it exposed details about their users' lives without getting the required legal consent. Last year, an independent audit that was part of the settlement found its privacy practices sufficient.

Despite criticisms, Facebook is rare among Internet companies in that it seeks user input on its privacy policy and tries to put it in plain English. But it also has a vast trove of data about its users that it uses to show ads and measure how well they work, among other things.

On Thursday, Facebook introduced a tool called "Privacy Basics," a set of animated, interactive guides designed to show users how to control what they share on the site. Tips answer questions such as "How do I delete something I post on Facebook?" or "What do people who aren't my friends see when they search for me?"

It also proposed changes to its terms and privacy policy, which it calls its data policy. The new policy is much shorter and lays out how Facebook collects data and what it does with it, among other things, in illustrated subsections.

Users will have seven days until Nov. 20 to comment on the new policy and the final version will go into effect soon after that.

The move comes as Facebook is testing a tool that lets users buy things through its site, and ramps up its ad targeting based on users' location. The new policy ensures that if people use Facebook to make a purchase, their credit card information will be collected, for example. Meanwhile, the location information Facebook collects might include where you took a photo that you share on the site, or the location of your mobile device using GPS, Bluetooth or WiFi signals.

A recent Pew Research Center poll found that some 80 percent of Americans who use social networking sites are concerned about third parties, such as advertisers, accessing data that they share on the sites. At the same time, most are willing to share some information about themselves in exchange for using such services for free.

WireLurker, Masque Attack Malware Only A Threat for Users Who Disable Apple's iOS, OS X Security

Despite headlines fretting of a "new era in OS X and iOS malware," Apple's security systems for iOS and OS X are working as intended to protect users from exposure to the ubiquitous malware affecting open platforms including Android and Windows. Here's the realistic, non-sensationalized facts about how safe Apple's users actually are and how users can remain protected from threats that arise.

Mac and iOS users are protected from viruses and malware by default unless the user bypasses their security systems, by jailbreaking an iOS device; by disabling the protections of Mac OS X's GateKeeper; or by choosing to "Trust" app installs that iOS identifies as being from an "Untrusted App Developer." Here's how those systems work, and how users can avoid being tricked into turning off their own security.

"WireLurker," a recent trojan horse attack detailed by Palo Alto Networks, was blocked in all forms even on Macs with key security features disabled by Apple within hours.

"We are aware of malicious software available from a download site aimed at users in China, and we've blocked the identified apps to prevent them from launching," Apple wrote in a statement last week.

Apple has previously used XProtect to remotely disabled user-installed Mac malware ("trojan horses," like the Russian Yontoo blocked last year) or software components with serious potential security vulnerabilities (such as Oracle Java), nipping problems in the bud before they could develop into an unmanageable security problem.

XProtect is so effective that the last significant malware issue for Macs (named Flashback) was a trojan horse masquerading as Adobe Flash Player that was specifically intended to disable XProtect (although the malware couldn't actually do this). WireLurker and Masque Attack aren't viral and can't infect users unless they intentionally disable their security and manually install apps bypassing Apple's builtin trust verification systems for iOS and Macs.

Masque Attack, a related exploit that shares one of the vulnerability vectors exploited by WireLurker, similarly requires users to "Trust" a request to install software from an unknown source, a step that Apple has now made effortlessly easy. Fortunately, users who inadvertently trust such apps from Untrusted Developers can review their iOS Provisioning Profiles to disable any self-signed certificates they have already approved.

WireLurker and Masque Attack are not viral and can't infect users unless they intentionally disable their security and manually install apps bypassing Apple's builtin trust verification systems for iOS and Macs.

That hasn't stopped sensational blogs from confusing users about how safe they actually are. Chris Smith, writing for BGR, spent paragraphs trying to convince readers that a minor distribution of Chinese malware "should terrify you," even though the identified malware has been circulating for months in China without actually delivering a real payload of malware outside of the wide open world of jailbroken devices.

Mac and iOS users have no need to be "terrified," but should understand in general terms how Apple's security systems work so they can't be fooled into installing malware. This is becoming a more complex issue because Apple now makes it easier than ever to bypass security on iOS, although it still requires an explicit "Trust" approval from the user.

Ironically, just two years ago the Electronic Frontier Foundation was demonizing the on-by-default security of iOS and OS X as "Apple’s Crystal Prison" and an "elaborate misdirection," and called upon the company to provide a "simple, documented, and reliable way to drill into a settings menu, unlatch the gate of the crystal prison, and leave."

Evil ’Unicorn’ 0-day Windows Bug Lurking Since 1995: Patch It Now!

Researcher Robert Freeman has identified an 18-year-old, critical remotely-exploitable hole affecting all versions of Windows all the way back to Windows 95.

The vulnerability (CVE-2014-6332) rated a critical score of 9.3 in all versions of Windows and was described as a rare "unicorn-like" bug in Internet Explorer-dependent code that opens avenues for man in the middle attacks.

The bug bypasses Redmond’s lauded Enhanced Mitigation Experience Toolkit along with Enhanced Protected Mode sandbox in the flagship browser and was patched today some six months after it was reported, IBM’s Freeman said.

"This complex vulnerability is a rare, ’unicorn-like’ bug [that can be used by an attacker for drive-by attacks to reliably run code remotely and take over the user s machine," Freeman said.

"In this case, the buggy code is at least 19 years old and has been remotely exploitable for the past 18 years.

"In some respects, this vulnerability has been sitting in plain sight for a long time despite many other bugs being discovered and patched in the same Windows library (OleAut32)."

Freeman said it was a "matter of time" before corresponding attacks surfaced in the wild.

It was the inclusion of VBScript in Internet Explorer that made the browser the most likely candidate for an attackers, Freeman said.

The discovery of the vulnerability could lead researchers an attackers to probe for more data manipulation bugs which may have been equally overlooked by security types.

"These data manipulation vulnerabilities could lead to substantial exploitation scenarios from the manipulation of data values to remote code execution," he said.

It was difficult to exploit the bug, plugged as part of Microsoft’s Patch Tuesday that crushed a string of serious holes, in part because array element sizes were fixed.

The scant opportunity to place arbitrary data where VBScript arrays were stored on the browser heap and the enforcement of variant type compatibility matching further complicated attacks.

Attacks could be launched using existing public research including that

described by Freeman.

A separate critical hole (MS14-066) affecting Microsoft’s Secure Channel (SChannel) that implemented Secure Sockets Layer and Transport Layer Security protocols was also patched.

That flaw permitted remote code execution in all versions of Windows if attackers sent crafted packets to Windows servers. The patch fixed sanitisation issues in Schannel for crafted packets.

Redmond issued 14 patchesto fix holes across Windows, Office, and .NET while Adobe set out to plug 18 holes in Flash and Air that allowed attackers to hijack user machines by way of remote code execution.

New Windows Security Bug Leaves PCs Open to Hijackings

If you re reading this on a Windows computer, you ve got some downloading to do.

As reported by Gizmodo, a newly discovered security bug leaves some Microsoft Windows PCs open to remote hijackings, meaning that someone else could take control of your computer and do as they wish with the files on it.

Exactly which Windows systems are affected? Well, it s unfortunately a lot.

According to Microsoft, the affected software includes multiple builds of Windows Server (2003 and 2008), Windows Vista, Windows 7, and Windows 8/8.1.

The fix: To be safe, we recommend that all PC users run the Windows Update program found inside the Windows Control Panel to make sure all available patches have been downloaded and installed. Microsoft s support site can also offer more info and a direct download for the fix now.

Raspberry Pi Launches Model A+ Microcomputer With A Price Of Only $20

The Raspberry Pi Foundation is known for creating microcomputers that run on Linux, have a low cost and are built on a single board. Today the Raspberry Pi Foundation announced the Model A+ microcomputer, which is smaller and cheaper than its predecessor.

Here is a breakdown of the specifications of the new Model A+ compared to some of the other Pi models.

The Model A+ has a starting price of $20 and the Model A predecessor is $25. The dimensions of the Model A versus the Model A+ are 85.60 mm × 56.50 mm and 65 mm × 56.50 mm, respectively. Other Raspberry Pi models are known for being roughly the same size as the average credit card, but the Model A+ is much smaller.

The Model A+ and the Model A have the same Broadcom BRCM +0.78% BCM2835

system-on-a-chip (SoC) clocked at 700MHz. Both also have 256MB of RAM. If you want to have a Raspberry Pi microcomputer with more RAM, the Model B series has 512MB of RAM and has a starting cost of $35.

The Model A series of Raspberry Pi devices have only one USB port. If you want to use more than one USB device, then you will need to have a USB hub or buy a device in the Model B series. The Model B has 2 USB ports and the Model B+ has 4 USB ports.

The Model A series of Raspberry Pi devices do not have an Ethernet port. By cutting out the Ethernet network connection and extra USB ports, the Model A+ uses drastically lower power than any other Pi model. In fact, the Model A+ uses between 20-25% less power than the original Model A.

The A+ still has an HDMI port, audio/video jack, camera connector and microUSB power slot. It also has a DSI display port to connect the Raspberry Pi touch screen display. And there is a new audio circuit and power supply that makes the Model A+ run quieter as well.

For storage purposes, a microSD slot has been used in the Model A+ to replace the SD card slot in other Pi models. The microSD slot in the Model A+ has a better push-push slot format compared to the old friction-fit SD card socket used in other models.

The Model A+ has more GPIO pins than its predecessor. The A+ has 40 GPIO pins and the A has 26. The Model A+ is also compatible with the HAT (Hardware Attached on Top) standard, meaning that third party add-on boards can be attached to it. Examples of third party add-on boards include motor controllers, LEDs, LCDs and DACs.

Last month, the Raspberry Pi Foundation announced that they sold 3.8 million total units. That figure is up from 3 million units in June 2014 and 2 million units in October 2013, according to ZDnet.

If you want to purchase a Model A+, they are available at MCM for U.S. customers and Farnell for U.K. customers.

As Firefox Turns 10, Mozilla Trumpets Privacy

Mozilla pulled out the PR stops to trumpet the 10th anniversary of Firefox, and in celebration released an interim build of Firefox 33 that includes a new privacy tool and access to the DuckDuckGo search engine.

Firefox 1.0 was released on Nov. 9, 2004, at a time when Microsoft’s Internet Explorer had a stranglehold on the browser space, having driven Netscape - Firefox’s forerunner in many ways - out of the market two years before. Mozilla has been widely credited with restarting browser development, which had been moribund under IE.

Today’s Firefox 33.1 offered DuckDuckGo as a new pre-installed search engine choice, joining Amazon, Bing, Google, Yahoo and others.

"DuckDuckGo gives you search results without tracking who you are or what you search for," said Johnathan Nightingale, vice president of Firefox, in a blog post. "Other engines may use tracking to enhance your search results, but we believe that’s a choice you should get to make for yourself."

Nightingale did not mention Google by name as one of the engines that "use tracking," but Google is the default search engine for most Firefox installations. New installations of Firefox 33.1 retain Google as the default, and current users' choices remain unchanged.

He also called out a new feature, dubbed "Forget," that has been added to Firefox. "Forget gives you an easy way to tell Firefox to clear out some of your recent activity," Nightingale wrote.

Forget, which must be added to the toolbar by the user, serves as a substitute for the more complex private browsing feature - called "Private Window" in Firefox - and the browser's already-available "Clear Recent History," which retroactively eliminates traces of where users have gone and what they've done on the Web.

"Many of our users share a computer with friends or family, and it's easy to forget to open a private browsing window first; with Forget, clearing that information is quick, and easy to understand," Nightingale said.

The focus on privacy was not limited to Firefox.

Mozilla's CEO, Chris Beard, also introduced a new project, called "Polaris," that he described as "a new strategic initiative to bring together the best and brightest to explore new approaches to enhance privacy controls online."

Elsewhere, Mozilla spelled out Polaris, which has a pair of partners at the start: the Tor Project and the Center for Democracy and Technology (CDT). Mozilla will host its own Tor middle relays, anonymous servers that receive Tor traffic and pass it along in an effort to improve the Tor network's overall performance and increase its capacity.

Mozilla also said it is working on another privacy tool that would replace the lifeless "Do Not Track" initiative with something that "protects those users that want to be free from invasive tracking without penalizing advertisers and content sites that respect a user's preferences."

Mozilla had been a strong proponent of Do Not Track, and in 2013 even said it would take the more drastic step of automatically blocking all third-party cookies. The latter was scuttled after online advertisers accused Mozilla of harboring "techno-libertarians and academic elites who believe in liberty and freedom ... as long as they get to decide the definitions of liberty and freedom." Instead, Mozilla partnered with Stanford University's Center for Internet and Society to create something labeled the "Cookie Clearinghouse," or CCH.

The privacy drumbeat, whether the addition of DuckDuckGo or the wider-ranging Polaris, seems at odds with Mozilla's primary revenue source, Google. In 2012, Mozilla's deal with Google produced $274 million in revenue, or 88% of the organization's total income for the year.

Mozilla's deal with Google will expire before the end of the year: In December 2011, the companies announced a renewal.

"Mozilla is currently in the midst of negotiations," a company spokesman said today, but declined to identify the partner or partners it was negotiating with. "These discussions are subject to traditional confidentiality requirements and as such, we are not at liberty to disclose further details at this time."

Complicating matters for Mozilla is the significant decline of Firefox since the last agreement with Google. According to U.S.-based Net Applications, Firefox’s user share has fallen 36% since December 2011; Irish measurement vendor StatCounter, meanwhile, said Firefox’s usage share was down 26% during that same period.

Firefox 33.1 for Windows, OS X and Linux can be downloaded from Mozilla’s website. Users of the browser will receive the update automatically.

Why The U.S. Has Fallen Behind in Internet Speed and Affordability

America s slow and expensive Internet is more than just an annoyance for people trying to watch Happy Gilmore on Netflix. Largely a consequence of monopoly providers, the sluggish service could have long-term economic consequences for American competitiveness.

Downloading a high-definition movie takes about seven seconds in Seoul, Hong Kong, Tokyo, Zurich, Bucharest and Paris, and people pay as little as $30 a month for that connection. In Los Angeles, New York and Washington, downloading the same movie takes 1.4 minutes for people with the fastest Internet available, and they pay $300 a month for the privilege, according to The Cost of Connectivity, a report published Thursday by the New America Foundation s Open Technology Institute.

The report compares Internet access in big American cities with access in Europe and Asia. Some surprising smaller American cities Chattanooga, Tenn.; Kansas City (in both Kansas and Missouri); Lafayette, La.; and Bristol, Va. tied for speed with the biggest cities abroad. In each, the high-speed Internet provider is not one of the big cable or phone companies that provide Internet to most of the United States, but a city-run network or start-up service.

The reason the United States lags many countries in both speed and affordability, according to people who study the issue, has nothing to do with technology. Instead, it is an economic policy problem the lack of competition in the broadband industry.

 It s just very simple economics, said Tim Wu, a professor at Columbia Law School who studies antitrust and communications and was an adviser to the Federal Trade Commission. The average market has one or two serious Internet providers, and they set their prices at monopoly or duopoly pricing.

London $24
Seoul $28
Paris $31
Tokyo $34
Copenhagen $36
Prague $39
Kansas City $41
Toronto $41
Berlin $42
Dublin $47
Lafayette, La. $50
Washington, D.C. $52
Hong Kong $52

Los Angeles $54
Chattanooga, Tenn. $54
New York City $55
San Francisco $58
Bristol, Va. $60
Mexico City $110

For relatively high-speed Internet at 25 megabits per second, 75 percent of homes have one option at most, according to the Federal Communications Commission usually Comcast, Time Warner, AT&T or Verizon. It s an issue anyone who has shopped for Internet knows well, and it is even worse for people who live in rural areas. It matters not just for entertainment; an Internet connection is necessary for people to find and perform jobs, and to do new things in areas like medicine and education.

Stop and let that sink in: Three-quarters of American homes have no competitive choice for the essential infrastructure for 21st-century economics and democracy, Tom Wheeler, chairman of the F.C.C., said in a speech last month.

The situation arose from this conundrum: Left alone, will companies compete, or is regulation necessary?

In many parts of Europe, the government tries to foster competition by requiring that the companies that own the pipes carrying broadband to people s homes lease space in their pipes to rival companies. (That policy is based on the work of Jean Tirole, who won the Nobel Prize in economics this month in part for his work on regulation and communications networks.)

In the United States, the Federal Communications Commission in 2002 reclassified high-speed Internet access as an information service, which is unregulated, rather than as telecommunications, which is regulated. Its hope was that Internet providers would compete with one another to provide the best networks. That didn t happen. The result has been that they have mostly stayed out of one another s markets.

When New America ranked cities by the average speed of broadband plans priced between $35 and $50 a month, the top three cities, Seoul, Hong Kong and Paris, offered speeds 10 times faster than the United States cities. (In some places, like Seoul, the government subsidizes Internet access to keep prices low.)

The divide is not just with the fastest plans. At nearly every speed, Internet access costs more in the United States than in Europe, according to the report. American Internet users are also much more likely than those in other countries to pay an additional fee, about $100 a year in many cities, to rent a modem that costs less than $100 in a store.

Fallen behind? Third world countries laugh at America’s grossly overpriced, abysmally poor internet service. There is no place on the planet...

Ah, the joys of the free market: expensive internet and unaffordable health care. So glad we ain’t socialists.

Well, whatever the problem, I’m sure the incoming GOP senate will fix the problem, because their concern is clearly with the average...

More competition, better technologies and increased quality of service on wireline networks help to drive down prices, said Nick Russo, a policy program associate studying broadband pricing at the Open Technology Institute and co-author of the report.

There is some disagreement about that conclusion, including from Richard Bennett, a visiting fellow at the American Enterprise Institute and a critic of those who say Internet service providers need more regulation. He argued that much of the slowness is caused not by broadband networks but by browsers, websites and high usage.

Yet it is telling that in the cities with the fastest Internet in the United States, according to New America, the incumbent companies are not providing the service. In Kansas City, it comes from Google. In Chattanooga, Lafayette and Bristol, it comes through publicly owned networks.

In each case, the networks are fiber-optic, which transfer data exponentially faster than cable networks. The problem is that installing fiber networks requires a huge investment of money and work, digging up streets and sidewalks, building a new network and competing with the incumbents. (That explains why super-rich Google has been one of the few private companies to do it.)

The big Internet providers have little reason to upgrade their entire networks to fiber because there has so far been little pressure from competitors or regulators to do so, said Susan Crawford, a visiting professor at Harvard Law School and author of Captive Audience: Telecom Monopolies in the New Gilded Age.

There are signs of a growing movement for cities to build their own fiber networks and lease the fiber to retail Internet providers. Some, like San Antonio, already have fiber in place, but there are policies restricting them from using it to offer Internet services to consumers. Other cities, like Santa Monica, Calif., have been laying fiber during other construction projects.

In certain cities, the threat of new Internet providers has spurred the big, existing companies to do something novel: increase the speeds they offer and build up their own fiber networks.

Facebook Now Lets You Unfollow People, Pages, and Groups From One Place

Facebook today announced an update that gives you more control over what shows up in your News Feed. This functionality falls under what the social network refers to as feedback for its algorithm.

Previously, if you saw a story you re not interested in or didn t want to see, you could tap the arrow in the top-right corner of that story to hide it. That s not changing, but now when you hide a story, you ll be asked if you want to see less from that person or Page. If you choose to, you are then given yet another option: You can unfollow them if you don t want to see any of their stories in your News Feed.

The second part of today s update is that the News Feed settings page has been updated to let you change what you see. The page now shows a list of the top people, Pages, and Groups that you ve seen in your News Feed over

the past week:

You can choose to sort posts by people, Pages, or Groups, as well as see an overall summary. You can unfollow any person or entity here as well, so you don t see their stories in your News Feed. Best of all, you can see who and what you ve unfollowed in the past, in case you forget, and refollow them if you change your mind.

What you do in News Feed helps determine what you see in News Feed, Facebook emphasized today. You decide who you want to connect to, and what Pages and public figures you want to follow.

This is a very welcome update. While Facebook s News Feed uses an algorithm to figure what stories to show you, it s certainly far from perfect, and users have to make an effort to customize it. Today s updates won t change the fundamental way that the News Feed works, but it will give users more power so they can fix it for themselves.

The timing is no surprise. During the company s first Q&A with Mark Zuckerberg yesterday, in which the CEO said My goal was never to make Facebook cool, the News Feed was a hot topic.

Users asked why the News Feed doesn t provide an unfiltered view of everything (content overload is always Facebook s response), or why there aren t easily accessible filters on the main page (Zuckerberg noted that users can make friend lists but acknowledged the feature is not intuitive at all). These new features are a step in the right direction, even though they re horribly overdue.

Google Scrapped The Mysterious Barges Because of Fire Risk

Google s mysterious boats faced a horrid situation when they were destroyed after being taken as a fire hazard. These floating showrooms of the tech giant were seen in Portland and SF a year ago. The 250 foot barge of Google were little known by the experts and the people and hence, they captured acute attention of the media towards self. According to the rumors, the barges must have cost the company a great amount of $4 million.

Google answered smartly about the barges and referred them as the interactive medium to aware people about the new technology. The media attention, however, turned into a bizarre situation for the barges as they were called for dismantling and being sold as scrap.

In the beginning, it was thought that the fading away of the barges was due to money issues. Experts thought that the money involved in the construction of the barges must have led to the decision of dismantling them up.

The contractor of Google actually paused the project after the Coast Guard put forward some fire safety concerns. The acting chief of the organization wrote in an email, These vessels will have over 5,000 gallons of fuel on the main deck and a substantial amount of combustible material on board.

Another visiting Coast guard added his concerns regarding the subject and said that some more safety measure needed to be employed in the case of

people jumping off board on the waterside. The Coast Guard officials raised their eyebrows over the matter and expressed their concern about the people with disabilities.

Google had assured the authorities that 150 people could be accommodated on the barge without any problem but the Coast guard did not buy it. Gauvin stated in an email, unaware of any measures you plan to use to actually limit the number of passengers, and while I understand there is a sense of urgency, I am concerned that significant work has already been performed without full consent of the Coast Guard.

Portland would have been on the winning side in any case, because they already collected $400,000 as a property tax. They would also lose out on some money in tourism due to the dismantling of the barges.

Facebook Will Be Mostly Video in 5 Years, Zuckerberg Says

If you think your Facebook feed has a lot of video now, just wait. In five years, most of [Facebook] will be video, CEO Mark Zuckerberg said Thursday during the company s first community town hall, in which he took questions from the public on a range of topics.

He was responding to a question about whether the growing number of photos uploaded to Facebook is putting a drag on its infrastructure. But Facebook s data centers have it covered, he said. The real challenge is improving the infrastructure to allow for more rich media like video in people s feeds.

Zuckerberg took questions from a group of users who were invited to its headquarters in Menlo Park, California, and people also submitted questions online.

One of the most popular online question was why Facebook forced users to download its Messenger app for mobile.

The 30-year-old acknowledged not everyone was thrilled with the change. Asking everyone in our community to install another app is a big ask, he said. But Facebook thought it could provide a better, faster messaging product if it split it off from its own app.

We really believe this is a better experience, Zuckerberg said. One user in the audience asked him if Facebook is losing its charm or becoming boring.

The question of Facebook losing its cool gets raised from time to time, Zuckerberg said, but my goal was never to make Facebook cool, he said. Instead, he wants it to be a helpful service that just works.

Another asked why he always seems wear the same t-shirts and hoodies. Zuckerberg said he wants to spend as much time as possible on things that matter, like how to build products, even if it means thinking less about what he wears.

Steve Jobs had the same approach, he said.

=~=~=~=